FINANCIAL INSTITUTION INFORMATION SECURITY
&
ROLE OF DIGITAL SIGNATURES

James M. Brundy
April 28, 2001

I. INTERNET SECURITY ISSUES FOR FINANCIAL INSTITUTIONS

A. Internet is inherently less secure than other means of remote communication.

1. Internet is a "packet-switched" network and is easier to penetrate than a private-line or software-defined private network.

2. World Wide Web servers that host sites have been shown to contain security lapses. Although "fixes" exist for many of these, the fixes are by no means universally installed.

3. World Wide Web browsers are easily attacked by "trojan horse" software that permits intruders to gather, e.g., password, account number and other private information from browsers in everyday use.

B. Known Security Issues[1]

1. Card number theft: penetration of several e-commerce sites resulting in theft of thousands of credit card numbers.

2. Identity theft: someone obtains the necessary information to pass themselves off as another… usually resulting in financial losses. The consequences often are expensive and time-consuming to correct.

3. Hacking of business, governmental and university computer systems.

4. Financial institutions ("FI's") are common and well-known targets for hackers, as "they're where the money is."

C. Financial Institution "Strategic Alliances."

1. FIs tend to lack sufficient expertise to bring their services to the Internet without assistance of outside specialists.

[1] Unlawful and undesirable conduct on the Internet is described in detail in PRESIDENT'S WORKING GROUP ON UNLAWFUL CONDUCT ON THE INTERNET, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USER OF THE INTERNET (2000).

2. Some FIs have had difficulty creating sufficiently rewarding environments to attract entrepreneurial, highly skilled and creative Internet technicians.

3. Creating "strategic alliances" with entrepreneurial companies provides FIs with access to Internet technologies and product suites that otherwise would be inaccessible.

4. "Strategic alliances" with these "dot.coms" often involve equity stakes by FIs, a practice that changes the dynamic from "vendor/ buyer" to "business partners." The FI acquiring services may be both advantaged, e.g., by closer collaboration, and disadvantaged, e.g., by the tendency to overlook matters that would have been taken seriously in the traditional environment.

D. "Dot.Com" Industry Immaturity; Effect of "Internet Speed."

1. By contrast to traditional information technology, e.g., mainframe computer services, insufficient time has passed to develop clear "best practices" for the "*.com" industry.

2. Management teams for "*.coms" tend to be less experienced, lacking knowledge of what characterizes an "industrial strength" business application.

3. "*.com" frequently must emphasize booking revenue at the expense of sustainability, reliability, security and other indicia of well-developed applications and well-managed services.

4. Emphasis on reducing "time to market" can lead to further cutting of corners on such indicia.

5. Operating at "Internet Speed," which tends to assume most innovations will be obsolete in 18 months or less, leads to additional pressure to minimize infrastructure investment.

E. Result perceived:

Security risks to FIs from service providers, especially those using Internet technology. One key risk perceived (among others) is unauthorized disclosure of confidential FI's customer information.

II. GRAMM LEACH BLILEY ACT ("GLBA") REQUIREMENTS

A. GLBA[2] § 501(a) states that "[I]t is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of

[2] 12 U.S.C. 6801, et. seq.

its customers and to protect the security and confidentiality of those customers' nonpublic personal information."

B. GLBA § 501(b) required the federal FI regulatory agencies[3] to "establish standards ... relating to administrative, technical and physical safeguards –

- "to insure the security and confidentiality of customer records and information;
- "to protect against any anticipated threats or hazards to the security or integrity of such records; and
- "to protect against unauthorized access to or use of such records or information which could result in substantial harm of inconvenience to any customer."

III. "INTERAGENCY GUIDELINES"

A. On June 26, 2000, the federal FI regulatory agencies issued for comment "Guidelines Establishing Standards for Safeguarding Customer Information …"[4] The final rule, published on February 1, 2001,[5] amended the regulations of each of the agencies to incorporate the Guidelines.[6] References hereafter are to the Appendix B to 12 C.F.R. Part 30, adopted by the Office of the Comptroller of the Currency ("OCC").

B. Information Security Program

Each FI must implement a comprehensive written information security program that implements the objectives of the GLBA (see ¶ II.B., above).[7]

1. The program applies to any record containing nonpublic personal information about an FI consumer customer[8], whether in paper, electronic

[3] The National Credit Union Administration (federally insured credit unions), the Securities and Exchange Commission (brokers and dealers, investment companies, investment advisers), State insurance authorities (persons engaged in providing insurance) and the Federal Trade Commission (any other financial institution) also were required to establish appropriate standards for the financial institutions subject to their respective jurisdictions. GLB Act. § 501(a).

[4] 65 FR 39472 (2000).

[5] 66 FR 8615 (2001).

[6] For example, the Office of the Comptroller of the Currency amended 12 C.F.R. Part 30 to incorporate an Appendix B that contains the Guidelines.

[7] 12 C.F.R. Part 30, Appendix B, ¶ II.A.

[8] "Customer has the same meaning as applies in the regulations implementing the privacy provisions of the GLB Act, i.e., a consumer who has a continuing relationship with an **FI** under

(… continued)

or other form.[9] However, the OCC subsequently "encouraged" national banks to extend the information security program to protect all customer and bank records.[10]

The decision to extend the program to all of the bank's records may be a momentous one. Not only does it significantly increase the expense of the program, but also it likely will require significant changes to the bank's operating procedures and service provider contracts.

2. The program must apply to physical, as well as electronic, records containing customer information in order to avoid such risks as "identity theft."

   It will be important to advise clients of the need to fold their existing information protection programs, typically designed to protect information on paper documents, e.g., shredding, secured waste paper disposal, etc., into the information security program implementing the Guidelines.

3. Not all parts of the organization, e.g., subsidiaries of a bank holding company, need have a uniform policy, but the policies must be coordinated.

C. Involvement By Board of Directors

The Board of Directors or a committee ("Directorate") must:

1. Approve the written information security program; oversee the development, implementation and maintenance of the program, including assigning specific implementation responsibility and reviewing management reports.[11]

2. The Directorate of each legal entity in the company, e.g., each bank holding company subsidiary, must carry out these responsibilities independently, although they all may adopt substantially the same program, as long as it complies with the requirements of the entity's primary supervisor.[12]

(… continued)
which the FI provides financial products to be used primarily for personal, family or household purposes. (12 C.F.R. Part 40, §§ 40.3(h) and (i)(1)).

[9] 12 C.F.R. Part 30, Appendix B, ¶ I.C.2.c.

[10] OCC Bulletin 2001-8 at 2.

[11] 12 C.F.R. Part 30, Appendix B, ¶ III.A.

[12] 66 F.R. 8620 (2001).

D. Activities in the Information Security Program

1. Assess Risk[13]

(a) The risk assessment must cover potential threats to customer information and customer information systems. This is a very broad charter, as "customer information systems" are any methods used to collect, process, store, transmit, protect or dispose of customer information.[14]

(b) The FI must evaluate the seriousness of these threats in light of the sensitivity of the customer information to be protected.[15]

2. Manage and Control Risk

(a) The FI must design its program to control the risks, commensurate with the sensitivity of the information and the complexity and scope of the FI's activities.[16]

(b) The Guidelines list eight measures that FIs must consider in determining their risk control strategy. These measures range from access controls and physical access restrictions through data encryption, change control procedures for information systems, monitoring to detect attacks/intrusions into the systems, response procedures to security breaches and disaster recovery planning.[17]

The federal FI regulators do not intend that each FI must implement the eight measures, it will likely be necessary for the FI to establish that it has considered each of them and made a sound decision whether or not to implement.

(c) The FI must regularly test the key controls. Tests should be conducted or reviewed by independent third parties or independent internal auditors.[18]

3. Oversee Service Provider Arrangements. FIs must:

(a) exercise due diligence in selecting service providers[19], including reviewing the measures taken by the service provider and any subservicer to protect customer information.[20]

---

[13] 12 C.F.R. Part 30, Appendix B, ¶ III.B.
[14] 12 C.F.R. Part 30, Appendix B, ¶ I.C.2.d.
[15] 12 C.F.R. Part 30, Appendix B, ¶ III.B.2.
[16] 12 C.F.R. Part 30, Appendix B, ¶ III.C.1.
[17] Id.
[18] 12 C.F.R. Part 30, Appendix B, ¶ III.C.3.

(b) require service providers by contract to implement appropriate measures designed to meet the objectives of the Guidelines.[21] Contracts entered into starting March 5, 2001 must contain this requirement. All other service provider contracts must be in compliance by July 1, 2003.[22]

The FI does not need to require a service provider to implement the program adopted by the FI. Indeed, when the provider services a number of FIs, it would likely be impossible to do so. However, each FI must satisfy itself that the service provider's program and plan applicable to the FI fulfills the objectives of the Guidelines.[23]

(c) monitor service provider information security programs to verify compliance, such as by reviewing audits, summaries of test results, etc.[24]

Obtaining the results of a SAS 70 audit of the service provider conducted at least annually by outside audit professionals could be sufficient in many cases to fulfill this requirement. Service providers to many FIs may have to insist on a process of this type, as it would be infeasible for them to allow each FI to conduct an audit.

4. Adjust the Program. FIs must take into account relevant changes in technology, sensitivity of customer information, internal and external threats and the FI's own changing corporate situation.[25]

5. Report to the Board. FIs must report to their Boards of Directors at least annually.[26]

E. Effective Date

1. The Guidelines became effective March 5, 2001.

2. FIs must have their information security programs in place by July 1, 2001.[27]

(… continued)

[19] 12 C.F.R. Part 30, Appendix B, ¶ III.D.1.
[20] 66 FR 8624 (2001).
[21] 12 C.F.R. Part 30, Appendix B, ¶ III.D.2.
[22] 12 C.F.R. Part 30, Appendix B, ¶ III.G.2.
[23] 66 FR 8624 (2001).
[24] 12 C.F.R. Part 30, Appendix B, ¶ III.D.3.
[25] 12 C.F.R. Part 30, Appendix B, ¶ III.E.
[26] 12 C.F.R. Part 30, Appendix B, ¶ III.F.

IV. OTHER REGULATORY GUIDANCE

The federal FI regulators have issued other relevant guidance to FIs on the subject of information protection. A sampling of these issuances is noted.[28]

(… continued)

[27] 12 C.F.R. Part 30, Appendix B, ¶ III.G.1.

[28] OCC Bulletin 2000-14, Infrastructure Threats – Intrusion Risks. Provides guidance on how to prevent, detect and respond to intrusions into bank computer systems. (May 15, 2000)
OCC Advisory Letter 2000-12, Risk Management of Outsourcing Technology Services. Transmits guidance from the Federal Financial Institutions Examination Council ("FFIEC") outlining the processes banks should use to manage the risks associated with outsourcing technology. (November 28, 2000)
OCC Bulletin OCC 99-20, Certification Authority Systems. Identifies the risks of certification authority systems. (May 4, 1999)
OCC Banking Circular BC-229, Information Security. Alerts management to the importance of information security. (May 31, 1998)
OCC Bulletin OCC 98-3, Technology Risk Management. Provides guidance on how national banks should identify, measure, monitor and control risks associated with the use of technology. (February 4, 1998)
OCC Bulletin OCC 97-3, FFIEC Interagency Statement on Corporate Business Resumption and Contingency Planning. Transmits the FFIEC policy statement of the same title explaining the goals of an effective business resumption and contingency plan.
OCC Banking Circular BC-226, End-User Computing. Transmits a joint issuance of the FFIEC on risks associated with end-user computing activities. (January 25, 1988)
OCC Advisory Letter AL 96-1, Document Security. Discusses appropriate procedures to ensure the security of confidential documents. (March 15, 1996)
OCC Banking Circular BC-187, Financial Information on Data Servicers Processing. Alerts national banks to the importance of performing financial reviews of organizations providing data processing services. (January 18, 1985)
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM ("FRB"), Supervisory Letter, SR 00-4(SUP), Outsourcing of Information and Transaction Processing. (February 29,2000).
FEDERAL DEPOSIT INSURANCE CORPORATION ('FDIC"), Financial Institution Letter FIL-67-2000, Security Monitoring of Computer Networks. (October 3, 2000)
FDIC, Financial Institution Letter FIL-131-97, Security Risks Associated with the Internet. (December 18, 1997)
OFFICE OF THRIFT SUPERVISION ("OTS"), Memorandum, Transactional Web Sites. Provides information on regulatory requirements for transactional web sites. (June 10, 1999)
OTS, Memorandum, Policy Statement on Privacy and Accuracy of Personal Customer Information. Set out "best practices" to adequately protect personal information. (November 3, 1998)
OTS, Memorandum, Statement on Retail On-Line Personal Computer Banking. Alerts to some of the risks and concerns of retail on-line PC banking. (June 23, 1997)

(… continued)

V. DIGITAL SIGNATURES

A. Digital signatures are a technology for encrypting digital transmissions.

1. This technology:

(a) ensures that the transmission is not changed en route (integrity),

(b) provides assurance that the sender actually is who she purports to be (attribution/authenticity), because the public key is included in a "certificate" issued by a trusted third party that is part of the digital signature. The third party issues the certificate to the sender after establishing her identity, and

(c) makes it very difficult to claim the transmission was sent by an impostor (non-repudiation).

With the addition of a date-stamp on the transmission, the time of sending can be established, as well.

2. This technology (sometimes called "public key infrastructure" or "PKI") achieves these objectives in large part by:

(a) encrypting certain unique information about the transmission, including, sometimes, the message itself, with a secret, "private key" known only to the sender;

(b) including in the encrypted transmission a "message digest," created by the sender, that is unique to the particular transmission;

(c) requiring use of the sender's "public key," which may be widely publicized, to <u>decrypt</u> the transmission; and

(d) recalculating the "message digest," to verify that it is the same as the sender inserted in the transmission.

3. This encryption/decryption relationship achieves the three characteristics described above (¶ V.A.1.) by:

(a) verifying the "message digest." If the transmission has been altered in any way en route, the "message digest" the receiver calculates will not match that sent,

---

(… continued)
OTS, Memorandum, <u>Risk Management of Client/Server Systems</u>. Encourages development and implementation of sound policies, practices and procedures to mitigate risks posed by a client/server environment. (October 24, 1996)

(b) relying on the certification by the trusted third party that the sender is who she purports to be, and

(c) determining that the sender's private key has not been compromised, so that only the sender could have encrypted the transmission.

B. Digital signatures provide high security for transmissions. No doubt, their use would fulfill any direction of the Guidelines to encrypt (see ¶ III.D.2(b) above). However, PKI systems are expensive and complex to create, manage and use. As a general mechanism for ensuring security of information transmitted, they may be "overkill" at this stage in their development.

C. Digital signatures can solve some practical problems arising in the use of electronic signatures in e-commerce transactions.

VI. ELECTRONIC SIGNATURES

A. Within the last two years many states have adopted the Uniform Electronic Transactions Act ("UETA") drafted by the National Conference of Commissioners on Uniform State Laws ("NCCUSL") and recommended by it for adoption at its July, 1999 meeting.[29]

B. On June 30, 2000 the federal Electronic Signatures in Global and National Commerce Act ("E-Sign")[30] became law amid much fanfare. This statute is modeled to some extent on UETA. It defers to state law in many respects if the states have adopted UETA in the version recommended by NCCUSL.

C. In each statute the fundamental proposition is that a record or signature cannot be denied legal effect simply because it is electronic.[31]

---

[29] The text of UETA is available at http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.htm.
[30] The text of E-Sign is available at http://thomas.loc.gov/cgi-bin/query/C?c106:./temp/~c106o8msSn.
[31] UETA § 7 reads: **"**SECTION 7. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS."(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
"(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.
"(c) If a law requires a record to be in writing, an electronic record satisfies the law.
"(d) If a law requires a signature, an electronic signature satisfies the law."

E-Sign § 101(a) reads: "(a) IN GENERAL- Notwithstanding any statute, regulation, or other rule of law (other than this title and title II), with respect to any transaction in or affecting interstate or foreign commerce--

(… continued)

D. The definitions of an "electronic signature" in E-Sign and UETA are almost identical.

1. E-Sign: ELECTRONIC SIGNATURE- The term `electronic signature' means an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.

2. UETA: "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

E. Neither statute provides much guidance regarding the practical use of an electronic signature. Among the issues that must be resolved are

1. What is the operational meaning of "attached to or logically associated with?" May the signature be a separate attachment? What constitutes a "logical association?"

2. How does one "execute or adopt?"

3. To what person is the signature attributable?

4. How is the intent to sign demonstrated?

These are primarily issues of proof.

F. Example: A user of a Website must agree to the site's terms of service ("TOS") containing liability allocations before entering the site. The user does this by clicking on a button labeled "I agree." When the site owner seeks to invoke the liability provisions, the named user denies having "clicked."

1. How can it be shown that the parties have agreed to contract electronically, so that UETA and E-Sign apply? This may be the easiest of all, as both UETA and E-Sign[32] provide that this agreement can be shown by all the surrounding circumstances.

(… continued)
"(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
"(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."

[32] Senate Report on S. 761, the Senate version of E-Sign, available at http://thomas.loc.gov/cgi-bin/cpquery/z?cp106:sr131, states in its analysis of § 6: "Subsection (b) does not require parties to enter into a separate agreement regarding their use of electronic

(… continued)

2. Is the button sufficiently "logically associated with" the TOS? What if the user claims that the TOS he "clicked" on did not contain the liability allocation at issue?

3. How can it be shown that the named user actually was the person that "clicked?"

4. Is "clicking" on the "I Agree" button sufficient to demonstrate "intent to sign?"

5. How can it be proved in a legal proceeding that may occur years later what the user was shown and to which the site owner thought the user was agreeing?

G. Paragraph 9(a) of the UETA[33] addresses attribution; E-sign lacks a comparable provision. UETA ¶ 9(a) provides that showing the efficacy of the security procedure used to determine who was acting can show that the signature is attributable to that person.

H. Digital signatures provide a solution to many of these practical issues. It is an effective security procedure that provides a way of determining who was acting. Because digital signatures offer assurance of integrity of the transmission, authenticity of the signature and non-repudiation, they answer the questions posed in ¶ VI.E. above. Furthermore, the need to take the specific step (even if automated) of creating the digital signature, including obtaining and using the private/public key pair and certificate, are circumstances that would help to establish the user's "intent to sign."

VII. OTHER ELECTRONIC SIGNATURE METHODS

A. The questions in ¶ VI.E., above, are not so readily answered with respect to electronic signature methods other than digital signatures. For example, "click-

---

(… continued)
signatures and records before they may rely on agreed terms and conditions when contracting with one another. The provision is intended to ensure that parties have maximum flexibility in the use and acceptance of electronic signatures and electronic records in connection with commercial transactions affecting interstate commerce.
The UETA provision (¶ 5(b)) is highly similar, and Official Comment 4 on UETA § 5 contains much the same language as just quoted.

[33] SECTION 9. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.
(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

through" methodologies are discussed specifically in the commentary to UETA § 9,[34] which stresses the need for security methods (passwords, user identification, etc.) as part of the proof necessary for attribution.

B. Counseling Considerations: When advising implementation of an electronic signature, consider what records would be necessary to provide the necessary evidence to demonstrate, after the passage of some time, that the user (or someone obtaining access with his consent) was the only person who could have signed the record.

- How can it be shown that another person could not have obtained access and initiated the transaction at issue without signing?

- How will the efficacy of the security procedure be proved after the passage of some time?

How can it be proved exactly what the user observed and agreed to prior to executing the process that created the "signature?"

[34] Official Comment 5 to UETA § 9.